(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11154184 A**

(43) Date of publication of application: **08.06.99**

(51) Int. Cl **G06F 17/60**
G06F 15/00
// G09C 1/00

(21) Application number: **09322833**

(22) Date of filing: **25.11.97**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT> NTT ELECTORNICS CORP**

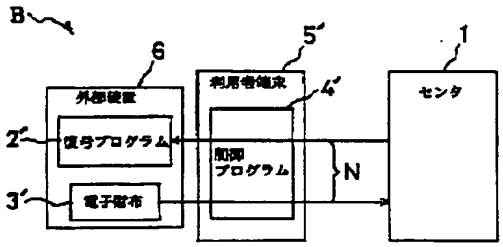
(72) Inventor: **TAKADA SHUNSUKE**
KAWAKUBO HIDEJI
YAMANAKA KIYOSHI
MATSUMOTO HIROYUKI

(54) **METHOD AND SYSTEM FOR MANAGING SAFETY OF INFORMATION DISTRIBUTION**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method and a system for managing safety of information distribution with which contents can be safely delivered and utilized in the information distribution in electronic commercial transaction.

SOLUTION: A center 1 having an enciphered distribution sales function, advertisement and propaganda function and payment collection settlement function and a user terminal 5' having a control program 4' for controlling an enciphered distribution purchase function, transfer function and drawing-out/ payment enciphering function are mutually connected by an information communication network N, and an external device 6 having a deciphering program 2' for deciphering enciphered sales contents Ke [M], which is transferred from the user terminal 5', with a previously or simultaneously transferred content cryptographic key Kup [Ke] enciphered in advance by operating while being interlocked with the control program 4', electronic wallet 3' for updating, enciphering and storing the payment subtracted remainder, and function for enciphering and storing various kinds of information is separately connected to the user terminal 5'.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－154184

(43)公開日　平成11年(1999)６月８日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	17/60		Ｇ０６Ｆ	15/21	３３０
	15/00	３３０		15/00	３３０Ｚ
// Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｆ
					６６０Ｂ

審査請求　未請求　請求項の数24　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－322833

(22)出願日　平成９年(1997)11月25日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(71)出願人　591230295
エヌティティエレクトロニクス株式会社
東京都渋谷区桜丘町20番１号

(72)発明者　高田　俊介
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　河久保　秀二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　菅　隆彦

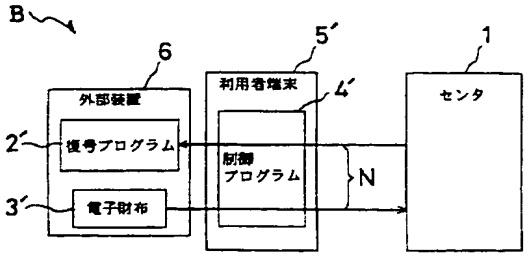
最終頁に続く

(54)【発明の名称】　情報流通安全管理方法及びシステム

(57)【要約】

【課題】電子商取引の情報流通において、コンテンツを安全に配送し利用し得る情報流通安全管理方法及びシステムの提供。

【解決手段】暗号化流通販売機能と広告宣伝機能と代金回収決算機能を有するセンタ１と、暗号化流通購入機能と転送機能と代金引出し支払い暗号化機能を制御する制御プログラム４′を有する利用者端末５′と間を情報通信網Ｎで相互接続し、制御プログラム４′に連携作動して利用者端末５′から転送された暗号化販売コンテンツＫｅ［Ｍ］を先又は同時に転送され事前に復号化されたコンテンツ暗号鍵Ｋｕｐ［Ｋｅ］で復号化処理する復号プログラム２′と、代金差引残高を更新暗号化記憶する電子財布３′と、各種情報の暗号化記憶機能と、を有する外部装置６を利用者端末５′に分離接続するシステム構成の特徴。



1

【特許請求の範囲】

【請求項１】販売コンテンツを有するセンタから情報通信網を介して店頭公開流通された広告宣伝用コンテンツ情報を利用者端末手段でアクセス閲覧して前記センタに購入要求し、当該利用者端末手段に配送された暗号化販売コンテンツの復号化処理及び電子決算処理の一連の電子商取引を行うに当り、

当該復号化処理及び当該電子決算処理の内の電子財布保管処理は、前記利用者端末と切離し、相互にプログラム連携して安全確保された外部処理に委ねられる、

ことを特徴とする情報流通安全管理方法。

【請求項２】店頭公開された広告宣伝用コンテンツ情報は、

情報購買意欲を湧かせるために、販売コンテンツが容易に推測出来、かつネットワーク負荷が小さい再編情報である、

ことを特徴とする請求項１に記載の情報流通安全管理方法。

【請求項３】センタ及び利用者端末は、

一連の電子商取引に公開鍵暗号方式を利用する、

ことを特徴とする請求項１又は２に記載の情報流通安全管理方法。

【請求項４】センタ及び利用者端末は、

それぞれ自己の秘密鍵を自己保持し、自己の公開鍵を相手に公開する、

ことを特徴とする請求項３に記載の情報流通安全管理方法。

【請求項５】配送された暗号化販売コンテンツは、

配送時に配送毎にランダムに生成されたコンテンツ暗号鍵で暗号化する、

ことを特徴とする請求項１、２、３又は４に記載の情報流通安全管理方法。

【請求項６】相互のプログラム連携は、

利用者端末の制御プログラムと外部処理の復号プログラム及び電子財布間で行われる、

ことを特徴とする請求項１、２、３、４又は５に記載の情報流通安全管理方法。

【請求項７】電子財布は、

電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保管する、

ことを特徴とする請求項６に記載の情報流通安全管理方法。

【請求項８】販売コンテンツは、

文書情報、画像情報、音声情報、これらの組合せ情報である、

ことを特徴とする請求項１、２、３、４、５、６又は７に記載の情報流通安全管理方法。

【請求項９】復号化処理は、

復号鍵及び秘密鍵を漏洩させない機密保護領域内で実行

2

される、

ことを特徴とする請求請１、２、３、４、５、６、７又は８に記載の情報流通安全管理方法。

【請求項１０】外部処理は、

マネー、コンテンツ、コンテンツ暗号鍵及び秘密鍵の全情報をマスター鍵にて機密保護領域内で暗号化されて記憶する、

ことを特徴とする請求項１、２、３、４、５、６、７、８又は９に記載の情報流通安全管理方法。

【請求項１１】マスター鍵は、

機密保護領域内に記憶保持される、

ことを特徴とする請求項１０に記載の情報流通安全管理方法。

【請求項１２】マネー、コンテンツ、暗号鍵及び秘密鍵の全情報は、

機密保護領域外に記憶保持される、

ことを特徴とする請求項１０又は１１に記載の情報流通安全管理方法。

【請求項１３】センタは、

ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含む、

ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１又は１２に記載の情報流通安全管理方法。

【請求項１４】情報通信網は、

インターネット、イントラネット（販売部を有する）、ＬＡＮ、ＶＡＮ、ＩＳＤＮ、ＶＰＮ等を含む、

ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２又は１３に記載の情報流通安全管理方法。

【請求項１５】センタ側では予め販売コンテンツを登録して置くステップ１（ＳＴ１）と、

当該販売コンテンツに基づき広告宣伝用コンテンツ情報を再編生成するステップ２（ＳＴ２）と、

当該広告宣伝用コンテンツ情報を利用者端末向に店頭公開するステップ３（ＳＴ３）と、

利用者端末でアクセス操作して当該広告宣伝用コンテンツ情報を閲覧するステップ４（ＳＴ４）と、

検討の上前記センタに購入要求するステップ５（ＳＴ５）と、

購入要求を受けた当該センタは乱数表等にて暗号鍵を生成するステップ６（ＳＴ６）と、

当該暗号鍵で前記販売コンテンツを暗号化処理するステップ７（ＳＴ７）と、

当該暗号化販売コンテンツと公開鍵で暗号化した当該暗号鍵を利用者端末に送信するステップ８（ＳＴ８）と、

当該暗号化販売コンテンツと当該暗号化暗号鍵とを受け

た利用者端末は外部処理に回すステップ９（ＳＴ９）と、
当該外部処理において、自己保持秘密鍵で復号化した前記暗号鍵で暗号化販売コンテンツを復号化処理してコンテンツを収得するステップ１０（ＳＴ１０）と、
前記外部処理で保管された電子財布から代金を利用者端末で引出して、前記センタに暗号化送信するステップ１１（ＳＴ１１）と、
代金を受信した前記センタは復号化決算処理するステップ１２（ＳＴ１２）と、
を順次踏んで実行処理する、
ことを特徴とする情報流通安全管理方法。
【請求項１６】販売コンテンツを登録し、広告宣伝用コンテンツを店頭公開流通するとともに購入要求に対し、公開鍵で暗号化したコンテンツ暗号鍵と当該コンテンツ暗号鍵で暗号化した販売コンテンツを送信して見返りに受信した代金を復号化決算処理するセンタと、
前記広告宣伝用コンテンツをアクセス閲覧して当該センタへ購入要求を応信し、返信してきた前記暗号化販売コンテンツと前記暗号化暗号鍵とを転信し、対価を引出して暗号化支払いを行う制御プログラムを有する利用者端末と、
前記センタと当該利用者端末を結ぶ情報通信網と、
前記制御プログラムに連携作動する復号プログラムと電子財布とを有し、前記利用者端末から転送されてきた前記暗号化コンテンツを、自己保持秘密鍵で復号化した前記暗号鍵で復号化し、再度暗号化記憶するとともに前記電子財布に記憶保持される電子マネーの代金差引残高を更新暗号化記憶する外部装置と、を備える、
ことを特徴とする情報流通安全管理システム。
【請求項１７】外部装置は、
暗号化コンテンツと暗号化コンテンツ暗号鍵を受信する端末入出力制御部と、
一連の復号、暗号及び記憶機能を統御する制御部と、
前記暗号化コンテンツ暗号鍵を自己保持秘密鍵で復号する暗号鍵復号部と、
前記暗号化販売コンテンツを当該コンテンツ暗号鍵でコンテンツに復号するコンテンツ復号部と、
マスター鍵を記憶保持するマスター記憶部と、
マネー、前記コンテンツ、前記コンテンツ暗号鍵及び前記秘密鍵の全情報を前記マスター鍵で暗号化又は復号化する暗号／復号部と、
暗号化された前記マネー情報を記憶するマネー情報記憶部と、
暗号化された前記コンテンツ情報を記憶するコンテンツ情報記憶部と、
暗号化された前記コンテンツ暗号鍵を記憶する暗号鍵記憶部と、
暗号化された前記秘密鍵を記憶する秘密鍵記憶部と、から構成される、
ことを特徴とする請求項１６に記載の情報流通安全管理システム。
【請求項１８】制御部とコンテンツ復号部とマスター鍵記憶部と暗号／復号部と暗号鍵復号部は、
外部装置に内蔵された機密保護装置内に収められている、
ことを特徴とする請求項１７に記載の情報流通安全管理システム。
【請求項１９】マネー情報記憶部は、
電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保持する機能を備える、
ことを特徴とする請求項１７又は１８に記載の情報流通安全管理システム。
【請求項２０】秘密鍵記憶部は、
公開鍵暗号方式の暗号化秘密鍵を記憶する機能を備える、
ことを特徴とする請求項１７、１８又は１９に記載の情報流通安全管理システム。
【請求項２１】コンテンツ情報記憶部は、
それぞれ暗号化文書情報、暗号化画像情報、暗号化音声情報、これ等の組合せ暗号化情報を記憶する機能を備える、
ことを特徴とする請求項１７、１８、１９又は２０に記載の情報流通安全管理システム。
【請求項２２】暗号鍵記憶部は、
暗号化コンテンツ暗号鍵を記憶する機能を備える、
ことを特徴とする請求項１７、１８、１９、２０又は２１に記載の情報流通安全管理システム。
【請求項２３】情報通信網は、
インターネット、イントラネット（販売部を有する）、ＬＡＮ、ＶＡＮ、ＩＳＤＮ、ＶＰＮ等を含む、
ことを特徴とする請求項１６、１７、１８、１９、２０、２１又は２２に記載の情報流通安全管理システム。
【請求項２４】センタは、
ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含む、
ことを特徴とする請求項１６、１７、１８、１９、２０、２１、２２又は２３に記載の情報流通安全管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、インターネット等の情報通信網を利用した情報流通安全管理方法及びその実施に直接使用するシステムに関する。
【０００２】
【従来の技術】従来の情報流通システムＡは図４に示す

よう、暗号化販売コンテンツ情報を店頭公開するセンタ１と、当該暗号化販売コンテンツ情報をアクセス閲覧し復号する復号プログラム２と、センタ１への送金用の電子財布３とを収めた制御プログラム４を保有する利用者端末５で構成される。

【０００３】当該情報流通システムＡの処理手順方法は、図５に示すようセンタ１側では、予め販売情報としてのコンテンツM情報を登録して置き（ＳＴＡ）、その都度暗号鍵Ｋｅを生成して（ＳＴＢ）、コンテンツMを暗号鍵Ｋｅで暗号化し（ＳＴＣ）、暗号化販売コンテンツＫｅ［M］を利用者端末５側に対し直接店頭公開する（ＳＴＤ）。

【０００４】次いで、利用者端末５側では、アクセス操作して暗号化販売コンテンツＫｅ［M］を閲覧し（ＳＴＥ）、制御プログラム４を駆動して、検討の上、購入要求をセンタ１に送信すれば（ＳＴＦ）、センタ１は受注を確認して暗号鍵Ｋｅを送信する（ＳＴＧ）。引続き、利用者端末５で暗号鍵Ｋｅを受けると復号プログラム２を駆動して保持していた暗号化販売コンテンツＫｅ［M］を暗号鍵Ｋｅで復号処理し、コンテンツMを得る（ＳＴＨ）。

【０００５】その上で、その対価支払いとして制御プログラム４により電子財布３からセンタ１向けに代金送信し（ＳＴＩ）、センタ１では、送金を受けて決算処理し（ＳＴＪ）、センタ１と利用者端末５間の電子商取引を終了する。

【０００６】

【発明が解決しようとする課題】以上の通り、従来の情報流通システムＡでは、予め原サイズコンテンツM情報の情報全部に特定の暗号鍵Ｋｅでモザイクや暗号化したコンテンツM情報を利用者に店頭公開し、利用者からの購入要求後に復号鍵Ｋｅを送信するため、容易に原サイズコンテンツM情報を推測出来ず、購買意欲が湧かないとともに、情報転送量が多く、最終的に利用者が購入しなかった場合の転送処理が無駄になり、しかも暗号鍵Ｋｅが盗まれると他の利用者が購入した該コンテンツM情報も不正利用される。

【０００７】又、利用者端末５内でコンテンツM情報を復号するため、利用者端末５や復号プログラム２に不正を行われると復号鍵Ｋｅが盗まれるとともに、利用者端末５内の購入コンテンツM情報を消去され、さらには電子クーポンやチケットなどの電子財布３情報を消去される危険を有する。

【０００８】ここにおいて、本発明の解決すべき主要な目的は次の通りである。即ち、本発明の第１の目的は、電子商取引の情報流通において、コンテンツを安全に配送し利用し得る情報流通安全管理方法及びシステムを提供せんとするものである。

【０００９】本発明の第２の目的は、電子商取引に先立って、電子広告宣伝し、購買意欲をそそって商売繁盛をもたらす情報流通安全管理方法及びシステムを提供せんとするものである。

【００１０】本発明の第３の目的は、販売コンテンツ情報に関する広告宣伝用コンテンツ情報に誇張化、書き換え等再編して店頭公開情報の転送量を少なくし合理化、効率化、経済化を計った情報流通安全管理方法及びシステムを提供せんとするものである。

【００１１】本発明の第４の目的は、利用者側の安全を要する復号処理及び電子マネー保管処理を利用者端末とは切離し連携した外部処理で行う情報流通安全管理方法及びシステムを提供せんとするものである。

【００１２】本発明のその他の目的は、明細書、図面、特に、特許請求の範囲の各請求項の記載から自ずと明かとなろう。

【００１３】

【課題を解決するための手段】本発明は、前記課題を解決するに当り、暗号化流通販売機能、広告宣伝機能及び代金回収復号化決算機能を有するセンタと、暗号化流通購入機能と転送機能と代金引出し暗号化支払い機能を制御する制御プログラムを有する利用者端末と間を情報通信網で接続し、前記制御プログラムに連携作動して前記利用者端末から転送された暗号化コンテンツを、先又は同時に転送され事前に復号化されたコンテンツ暗号鍵で復号化処理する復号プログラミングと代金差し引き残高を更新暗号化記憶する電子財布と，各種情報の暗号化記憶機能と，を有する外部装置を前記利用者端末に分離接続するシステム構成を採用する。

【００１４】そして、利用者に情報を店頭公開する際、情報購買意欲を湧かせるために原情報が容易に推測でき、かつサイズの小さい情報を公開するとともに、情報配送時に乱数表等にて生成したセッション鍵を暗号化する一方、情報復号を外部装置の機密保護装置で行い、復号鍵を漏洩させない。しかも、購入情報を外部装置に保持させ、電子マネーとして電子クーポンや電子チケット等の残高情報を外部装置内の電子財布に安全に保持する。

【００１５】さらに、具体的詳細に述べれば、本発明が、当該課題解決のため、次に列挙する上位概念から下位概念に亙る新規な特徴的構成手法又は手段を採用することにより、前記目的を達成する。

【００１６】即ち、本発明方法の第１の特徴は、販売コンテンツを有するセンタから情報通信網を介して店頭公開流通された広告宣伝用コンテンツ情報を利用者端末手段でアクセス閲覧して前記センタに購入要求し、当該利用者端末手段に配送された暗号化販売コンテンツの復号化処理及び電子決算処理の一連の電子商取引を行うに当り、当該復号化処理及び当該電子決算処理の内の電子財布保管処理は、前記利用者端末と切離し、相互にプログラム連携して安全確保された外部処理に委ねられてなる情報流通安全管理方法の構成採用にある。

【００１７】本発明方法の第２の特徴は、前記本発明方法の第１の特徴における店頭公開された広告宣伝用コンテンツ情報が、情報購買意欲を湧かせるために、販売コンテンツが容易に推測出来、かつネットワーク負荷が小さい再編情報である情報流通安全管理方法の構成採用にある。

【００１８】本発明方法の第３の特徴は、前記本発明方法の第１又は第２の特徴におけるセンタ及び利用者端末が、一連の電子商取引に公開鍵暗号方式を利用してなる情報流通安全管理方法の構成採用にある。

【００１９】本発明方法の第４の特徴は、前記本発明方法の第３の特徴におけるセンタ及び利用者端末が、それぞれ自己の秘密鍵を自己保持し、自己の公開鍵を相手に公開してなる情報流通安全管理方法の構成採用にある。

【００２０】本発明方法の第５の特徴は、前記本発明方法の第１、第２、第３又は第４の特徴における配送された暗号化販売コンテンツが、配送時に配送毎にランダムに生成されたコンテンツ暗号鍵で暗号化してなる情報流通安全管理方法の構成採用にある。

【００２１】本発明方法の第６の特徴は、前記本発明方法の第１、第２、第３、第４又は第５の特徴における相互のプログラム連携が、利用者端末の制御プログラムと外部処理の復号プログラム及び電子財布間で行われてなる情報流通安全管理方法の構成採用にある。

【００２２】本発明方法の第７の特徴は、前記本発明方法の第６の特徴における電子財布が、電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保持してなる情報流通安全管理方法の構成採用にある。

【００２３】本発明方法の第８の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６又は第７の特徴における販売コンテンツが、文書情報、画像情報、音声情報、これらの組合せ情報である情報流通安全管理方法の構成採用にある。

【００２４】本発明方法の第９の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６、第７又は第８の特徴における復号化処理が、復号鍵及び秘密鍵を漏洩させない機密保護領域内で実行されてなる情報流通安全管理方法の構成採用にある。

【００２５】本発明方法の第１０の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８又は第９の特徴における外部処理が、マネー、コンテンツ、コンテンツ暗号鍵及び秘密鍵の全情報をマスター鍵にて機密保護領域内で暗号化されて記憶してなる情報流通安全管理方法の構成採用にある。

【００２６】本発明方法の第１１の特徴は、前記本発明方法の第１０の特徴におけるマスター鍵が、機密保護領域内に記憶保持されてなる情報流通安全管理方法の構成採用にある。

【００２７】本発明方法の第１２の特徴は、前記本発明方法の第１０又は第１１の特徴におけるマネー、コンテンツ、暗号鍵及び秘密鍵の全情報が、機密保護領域外に記憶保持されてなる情報流通安全管理方法の構成採用にある。

【００２８】本発明方法の第１３の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１又は第１２の特徴におけるセンタが、ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含んでなる情報流通安全管理方法の構成採用にある。

【００２９】本発明方法の第１４の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２又は第１３の特徴における情報通信網が、インターネット、イントラネット（販売部を有する）、ＬＡＮ、ＶＡＮ、ＩＳＤＮ、ＶＰＮ等を含んでなる情報流通安全管理方法の構成採用にある。

【００３０】本発明方法の第１５の特徴は、センタ側では予め販売コンテンツを登録して置くステップ１（ＳＴ１）と、当該販売コンテンツに基づき広告宣伝用コンテンツ情報を再編生成するステップ２（ＳＴ２）と、当該広告宣伝用コンテンツ情報を利用者端末向に店頭公開するステップ３（ＳＴ３）と、利用者端末でアクセス操作して当該広告宣伝用コンテンツ情報を閲覧するステップ４（ＳＴ４）と、検討の上前記センタに購入要求するステップ５（ＳＴ５）と、購入要求を受けた当該センタは乱数表等にて暗号鍵を生成するステップ６（ＳＴ６）と、当該暗号鍵で前記販売コンテンツを暗号化処理するステップ７（ＳＴ７）と、当該暗号化販売コンテンツと公開鍵で暗号化した当該暗号鍵を利用者端末に送信するステップ８（ＳＴ８）と、当該暗号化販売コンテンツと当該暗号化暗号鍵とを受けた利用者端末は外部処理に回すステップ９（ＳＴ９）と、当該外部処理において、自己保持秘密鍵で復号化した前記暗号鍵で暗号化販売コンテンツを復号化処理してコンテンツを収得するステップ１０（ＳＴ１０）と、前記外部処理で保管された電子財布から代金を利用者端末で引出して、前記センタに暗号化送信するステップ１１（ＳＴ１１）と、代金を受信した前記センタは復号化決算処理するステップ１２（ＳＴ１２）と、を順次踏んで実行処理してなる情報流通安全管理方法の構成採用にある。

【００３１】本発明システムの第１の特徴は、販売コンテンツを登録し、広告宣伝用コンテンツを店頭公開流通するとともに購入要求に対し、公開鍵で暗号化したコンテンツ暗号鍵と当該コンテンツ暗号鍵で暗号化した販売コンテンツを送信して見返りに受信した代金を復号化決算処理するセンタと、前記広告宣伝用コンテンツをアク

セス閲覧して当該センタへ購入要求を応信し、返信してきた前記暗号化販売コンテンツと前記暗号化暗号鍵とを転信し、対価を引出して暗号化支払いを行う制御プログラムを有する利用者端末と、前記センタと当該利用者端末を結ぶ情報通信網と、前記制御プログラムに連携作動する復号プログラムと電子財布とを有し、前記利用者端末から転送されてきた前記暗号化コンテンツを、自己保持秘密鍵で復号化した前記暗号鍵で復号化し、再度暗号化記憶するとともに前記電子財布に記憶保持される電子マネーの代金差引残高を更新暗号化記憶する外部装置と、を備えてなる情報流通安全管理システムの構成採用にある。

【００３２】本発明システムの第２の特徴は、前記本発明システムの第１の特徴における外部装置が、暗号化コンテンツと暗号化コンテンツ暗号鍵を受信する端末入出力制御部と、一連の復号、暗号及び記憶機能を統御する制御部と、前記暗号化コンテンツ暗号鍵を自己保持秘密鍵で復号する暗号鍵復号部と、前記暗号化販売コンテンツを当該コンテンツ暗号鍵でコンテンツに復号するコンテンツ復号部と、マスター鍵を記憶保持するマスター記憶部と、マネー、前記コンテンツ、前記コンテンツ暗号鍵及び前記秘密鍵の全情報を前記マスター鍵で暗号化又は復号化する暗号／復号部と、暗号化された前記マネー情報を記憶するマネー情報記憶部と、暗号化された前記コンテンツ情報を記憶するコンテンツ情報記憶部と、暗号化された前記コンテンツ暗号鍵を記憶する暗号鍵記憶部と、暗号化された前記秘密鍵を記憶する秘密鍵記憶部と、から構成されてなる情報流通安全管理システムの構成採用にある。

【００３３】本発明システムの第３の特徴は、前記本発明システムの第２の特徴における制御部とコンテンツ復号部とマスター鍵記憶部と暗号／復号部と暗号鍵復号部が、外部装置に内蔵された機密保護装置内に収められてなる情報流通安全管理システムの構成採用にある。

【００３４】本発明システムの第４の特徴は、前記本発明システムの第２又は第３の特徴におけるマネー情報記憶部が、電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の暗号化残高情報を記憶保持する機能を備えてなる情報流通安全管理システムの構成採用にある。

【００３５】本発明システムの第５の特徴は、前記本発明システムの第２、第３又は第４の特徴における秘密鍵記憶部が、公開鍵暗号方式の暗号化秘密鍵を記憶する機能を備えてなる情報流通安全管理システムの構成採用にある。

【００３６】本発明システムの第６の特徴は、前記本発明システムの第２、第３、第４又は第５の特徴におけるコンテンツ情報記憶部が、それぞれ暗号化文書情報、暗号化画像情報、暗号化音声情報、これ等の組合せ暗号化情報を記憶する機能を備えてなる情報流通安全管理システムの構成採用にある。

【００３７】本発明システムの第７の特徴は、前記本発明システムの第２、第３、第４、第５又は第６の特徴における暗号鍵記憶部が、暗号化コンテンツ暗号鍵を記憶する機能を備えてなる情報流通安全管理システムの構成採用にある。

【００３８】本発明システムの第８の特徴は、前記本発明システムの第１、第２、第３、第４、第５、第６又は第７の特徴における情報通信網が、インターネット、イントラネット（販売部を有する）、ＬＡＮ、ＶＡＮ、ＩＳＤＮ、ＶＰＮ等を含んでなる情報流通安全管理システムの構成採用にある。

【００３９】本発明システムの第９の特徴は、前記本発明システムの第１、第２、第３、第４、第５、第６、第７又は第８の特徴におけるセンタが、ストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社、出版社、放送局、レコード会社、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含んでなる情報流通安全管理システムの構成採用にある。

【００４０】

【発明の実施の形態】本発明の実施の形態をその方法例及びシステム例につき図面を参照して説明する。本実施形態例では、文書情報や画像情報や音声情報やこれ等の組合せ情報の販売コンテンツをホームページ等を開設するストアやショップ、ショッピングセンタ、コミュニケーションセンタ、ショッピングモール、図書館、資料館、雑誌社出版社、放送局、ゲームソフト会社、映画会社、新聞社等のヴァーチャル及びリアルを含むセンタから、インターネット、イントラネット（販売部を有する）、ＬＡＮ、ＶＡＮ、ＩＳＤＮ、ＶＰＮ等を含む情報通信網のネットワークシステムを通して、利用者端末に対し店頭公開するとともに、電子決算として電子クーポンや電子チケットや電子小切手やビットキャッシュやクレジットカードやサイバーコイン等の電子マネー残高を保管する電子財布を使用して電子商取引を行う場合を想定しているも、これに限定されるものではない。本発明の目的を達成し、後述する効果を有する範囲内においても適用可能である。

【００４１】（システム例）本実施形態のシステム例を図１乃至図２について説明する。図１は本システム例を示す情報流通安全管理システムのブロック概念構成図、図２は同・外部装置内部の詳細ブロック構成図である。

【００４２】本システムＢは、センタ１と制御プログラム４′を保有する利用者端末５′と、復号プログラム２′及び電子財布３′を保有する外部装置６とからなり、センタ１と利用者端末５′間は情報通信網Ｎで接続される。なお、図４の従来システム例Ａと同一構成ブロックは同一符号を付して説明の重複を避けた。

【００４３】前記センタ１は、販売コンテンツＭを品揃

え登録し、広告宣伝用コンテンツM′を店頭公開するとともに、購入要求に対し暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］と暗号化販売コンテンツＫｅ［M］をともども送信して見返りに受信した暗号化代金を復号化決算処理する機能を有する。

【００４４】前記利用者端末５′は、制御プログラム４′に則って広告宣伝用コンテンツM′をアクセス閲覧してセンタ１へ購入要求を応信し、返信して来た暗号化販売コンテンツＫｅ［M］と暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］とを転信し、対価引出し支払を暗号化送信する機能を有する。

【００４５】前記外部装置６は、制御プログラム４′に連携作動する復号プログラム２′と電子財布３′により、利用者端末５′から転送されて来た暗号化販売コンテンツＫｅ［M］を先に又は同時に転送され事前に復号化した暗号鍵Ｋｅで復号化記憶するとともに記憶保持される電子マネーの代金差し引き残高を更新暗号化記憶する機能を有する。

【００４６】それ故、当該外部装置６は、図２に示すよう、暗号化販売コンテンツＫｅ［M］と暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］を受信する端末入出力制御部７と、一連の復号、暗号及び記憶機能並びに代金差し引き残高保管記憶機能を統御する制御部８と、暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］を復号する暗号鍵復号部９と、暗号化販売コンテンツＫｅ［M］をコンテンツ暗号鍵Ｋｅで復号するコンテンツ復号部１０と、マスター鍵Ｋｍを記憶保持するマスター鍵記憶部１１と、マネー、コンテンツM、コンテンツ暗号鍵Ｋｅ及び秘密鍵Ｋｕｓの全情報をマスター鍵Ｋｍで暗号化又は復号化する暗号／復号部１２と、当該暗号化されたマネー情報を記憶するマネー情報記憶部１３と、当該暗号化されたコンテンツ情報Ｋｍ［M］を記憶するコンテンツ情報記憶部１４と、当該暗号化されたコンテンツ暗号鍵Ｋｍ［Ｋｅ］を記憶する暗号鍵記憶部１５と、当該暗号化された秘密鍵Ｋｍ［Ｋｕｓ］を記憶する秘密鍵記憶部１６とで内部構成され、制御部８と暗号鍵復号部９とコンテンツ復号部１０とマスター鍵記憶部１１と暗号／復号部１２は機密保護装置１７に不可侵安全に内蔵される。

【００４７】（方法例）当該本システム例に適用する本実施形態の方法例を図面について説明する。図３は本方法例の実行処理する手順動作シーケンスチャートである。

【００４８】（１）初期条件

センタ１は、公開鍵暗号方式の秘密鍵Ｋｃｓを持ち、公開鍵Ｋｃｐを公開している一方、利用者端末５′は公開暗号方式の秘密鍵Ｋｕｓを外部装置６に持ち、公開鍵Ｋｕｐを公開する。又、外部装置６の製造時には、機密保護装置１７内のマスター鍵記憶部１１に装置固有のマスター鍵Ｋｍを書き込む。

【００４９】他方、利用者端末５′の秘密鍵Ｋｕｓは、外部装置６の暗号／復号部１２において、マスター鍵記憶部１１に記憶してあるマスター鍵Ｋｍで暗号化し、当該暗号化された秘密鍵Ｋｍ［Ｋｕｓ］を秘密鍵暗号部１６に書き込み、その上で、センタ１は利用者登録し、ある一定額の金券等を利用者端末５′に送信し、利用者はマネー情報記憶部１３に暗号／復号部１２でマスター鍵Ｋｍにより暗号化してマネー情報記憶部１３に格納する。

【００５０】（２）センタ１の一次処理手順

まず、販売用のコンテンツMを登録して置く（ＳＴ１）。次いで、コンテンツMから利用者に無料で提供でき購買意欲を誘うような広告宣伝用コンテンツM′を生成する（ＳＴ２）。なお、情報提供者が広告宣伝用コンテンツM′を生成した後に、センタ１にコンテンツMを登録しても良い。広告宣伝用コンテンツM′は再編した、例えば、画像ならばサイズを小さくしたもの、ゲームならば体験版、音楽ならプログラム、映像ならば予告編版等のデータ転送の時間が余り掛からない程度のネットワークに負荷が小さいコンテンツM′とする。当該再編された広告宣伝用コンテンツM′を店頭公開する（ＳＴ３）。

【００５１】（３）利用者の一次処理手順

まず、流通広告宣伝用コンテンツM′を利用者端末５′でホームページ等を検索して閲覧する（ＳＴ４）。次いで、購入する場合は購入要求をセンタ１に送信する（ＳＴ５）。

【００５２】（４）センタ１の二次処理手順

利用者からの購入要求を受信すると、まず、コンテンツ暗号鍵Ｋｅを乱数表を用いてランダム生成する（ＳＴ６）。次いで、コンテンツMをコンテンツ暗号鍵Ｋｅで暗号化Ｋｅ［M］をする（ＳＴ７）。引続き、コンテンツ暗号鍵Ｋｅを利用者の公開鍵Ｋｕｐで暗号化したコンテンツ暗号鍵Ｋｕｐ［Ｋｅ］と暗号化販売コンテンツＫｅ［M］を利用者に送信する（ＳＴ８）。

【００５３】（５）利用者の二次処理手順

（手順例１）利用者端末５′が暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］と暗号化販売コンテンツＫｅ［M］を受信すると、制御プログラム４′はまず、暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］を外部装置６に転送し、次いで端末入出力制御部７は、コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］を転入し制御部８に引き渡す。

【００５４】引続いて、制御部８は以降本処理手順の最終まで連続して駆動し続ける復号プログラム２′に則り、秘密鍵記憶部１６に格納されている暗号化秘密鍵Ｋｍ［Ｋｕｓ］を暗号／復号部１２で復号し、暗号鍵復号部９において秘密鍵Ｋｕｓで暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］を復号する。制御部８は、暗号／復号部１２においてマスター鍵Ｋｍで暗号鍵Ｋｅを暗号化Ｋｍ［Ｋｅ］し、暗号鍵記憶部１５に格納する。

【００５５】他方、制御プログラム４′は暗号化販売コ

ンテンツＫｅ［M］を外部装置６に転送し、さらに、端末入出力制御部７は、暗号化販売コンテンツＫｅ［M］を転入し、制御部８に引き渡す。その上で、制御部８は、さらに駆動し続ける復号プログラム２′に則り、暗号鍵記憶部１５にある暗号化コンテンツ暗号鍵Ｋｍ［Ｋｅ］を暗号／復号部１２においてマスター鍵Ｋｍで復号した後、制御部８は、コンテンツ復号部１０において、取得した暗号鍵Ｋｅで暗号化販売コンテンツＫｅ［M］を復号し（ＳＴ１０）、取得したコンテンツMを暗号／復号部１２にてマスター鍵Ｋｍで暗号化しコンテンツ情報記憶部１４に記憶させると同時にコンテンツMを端末入出力制御部７から利用者端末５′に出力する。

【００５６】（手順例２）利用者端末５′が暗号化コンテンツ暗号鍵Ｋｕｐ［ｋｅ］と暗号化販売コンテンツＫｅ［M］を受信する（ＳＴ９）と、制御プログラム４′は、制御端末入出力制御部７を介して制御部８に暗号化コンテンツ暗号鍵Ｋｕｐ［Ｋｅ］と暗号化販売コンテンツＫｅ［M］を同時に転送し、そのまま暗号／復号部１２においてマスター鍵Ｋｍでさらに暗号化し、ダブル暗号化コンテンツ暗号鍵Ｋｍ｛Ｋｕｐ［Ｋｅ］｝とダブル暗号化販売コンテンツＫｍ｛Ｋｅ［M］｝とをそれぞれコンテンツ情報記憶部１４と暗号鍵記憶部１５に格納する。

【００５７】利用者は、コンテンツMを利用したい時に制御部８を動作して復号プログラム２′を駆動し、コンテンツ情報記憶部１５から読み出したダブル暗号化販売コンテンツＫｍ｛Ｋｅ［M］｝を暗号／復号部１２においてマスター鍵Ｋｍで復号化した後、一旦暗号化販売コンテンツＫｅ［M］を端末入出力制御部７に出力して一度利用者端末５′の制御プログラム４′に戻す。その後の手順は手順例１の［００５５］以降の処理を行う。

【００５８】（６）電子決算処理

利用者の二次処理手順が終了すると利用者端末５′の制御プログラム４′は外部装置６の制御部８に電子財布３′のマネー情報記憶部１３の電子マネー金券等残高を通知するよう命令して、読み出した暗号化金券等残高を暗号／復号部１２においてマスター鍵Ｋｍで復号した後、端末入出力制御部７を通して利用者端末５′に金券等残高情報が送られる。

【００５９】次いで、制御プログラム４′は、通常の電子クーポン処理や課金モジュールの処理によりセンタ１に公開鍵Ｋｃｐで暗号化した代金を送信し（ＳＴ１１）、コンテンツMの価格を差し引いた金券等残高情報を再度、外部装置６の端末入出力制御部７、制御部８、暗号／復号部１２を経由してマネー情報記憶部１３に更新格納する。他方、暗号化代金を送信されたセンタ１は、秘密鍵Ｋｃｓで復号し、コンテンツMの電子商取引に係わる決算処理（ＳＴ１２）を実行して電子商取引を完了する。

【００６０】

【発明の効果】かくして、本発明は、利用者端末側で制御プログラムを連携動作しかつ機密安全性を確保された外部装置の外部処理に復号解読と電子財布の管理を委ねるとともに、センタと、利用者端末間の情報流通を基本的には公開暗号鍵方式の採用の上で、情報配送時にセッション鍵で暗号化し、さらに外部装置の機密内領域の外部処理にマスター鍵を用いて本発明の電子商取引に三重安全管理体制を敷いて、情報流通における情報の安全保護を計る。

【００６１】しかも、電子商取引を行うため、コンテンツの販売に先立って現実社会の商取引における広告宣伝同様、引き合い閲覧に負担にならず、知恵の出し所となる広告宣伝用のコンテンツを店頭公開流通して利用者の注意を喚起して購買意欲をそそり、より多くの顧客吸引力を発揮した上で、多くの購入要求を事前に得てから現物コンテンツを配信引き渡す電子商取引の合理化、効率化、安全化及び経済化を達成する等優れた効果を奏する。

【図面の簡単な説明】

【図１】本発明の実施の形態を示すシステム例の概念ブロック構成図である。

【図２】同上における外部装置内部の詳細ブロック構成図である。

【図３】本発明の実施の形態を示す方法例を実行処理する手順動作のシーケンスチャートである。

【図４】従来システム例の概念ブロック構成図である。

【図５】従来方法例を実行処理する手順動作のシーケンスチャートである。

【符号の説明】

Ａ…従来システム例
Ｂ…本実施形態システム例
１…センタ
２，２′…復号プログラム
３，３′…電子財布
４，４′…制御プログラム
５，５′…利用者端末
６…外部装置
７…端末入出力制御部
８…制御部
９…暗号鍵復号部
１０…コンテンツ復号部
１１…マスター鍵記憶部
１２…暗号／復号部
１３…マネー情報記憶部
１４…コンテンツ情報記憶部
１５…暗号鍵記憶部
１６…秘密鍵記憶部
Ｋｃｓ，Ｋｕｓ…秘密鍵
Ｋｃｐ，Ｋｕｐ…公開鍵
Ｋｅ…コンテンツ暗号鍵

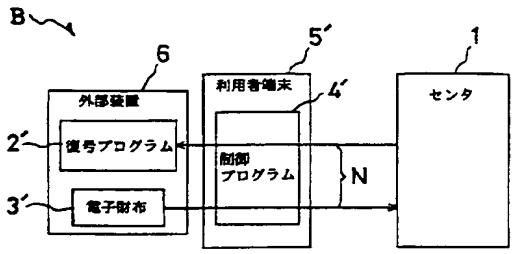
15

Ｋｅ［Ｍ］…暗号化販売コンテンツ
Ｋｍ…マスター鍵

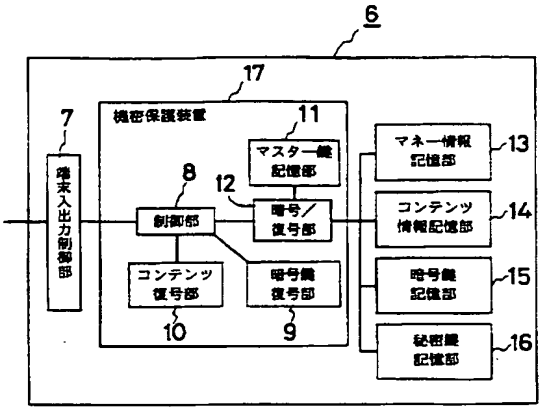
16

Ｍ…コンテンツ
Ｍ′…広告宣伝用コンテンツ

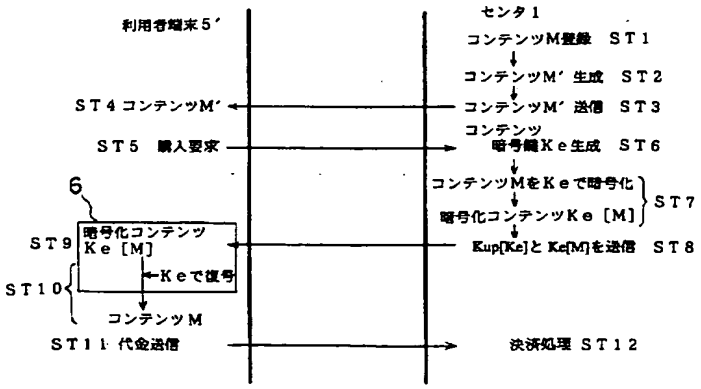
【図１】



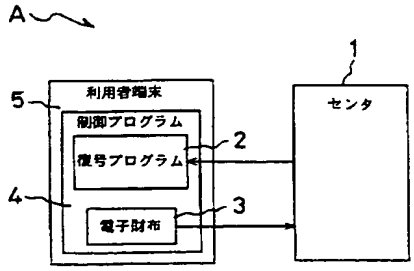
【図２】



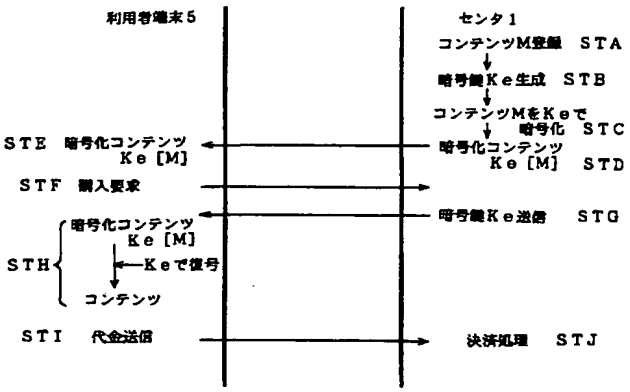
【図３】



【図４】



【図５】



フロントページの続き

(72)発明者　山中　喜義
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　松本　博幸
東京都渋谷区桜丘町20番１号　エヌティティエレクトロニクス株式会社内